REMARKS/ARGUMENTS

Favorable reconsideration of this application in light of the following discussion is respectfully requested.

Claims 9-17 are pending in the application. No claims are amended or added by the present amendment.

In the outstanding Official Action, Claims 9-17 were rejected under 35 U.S.C. § 103(a) as unpatentable over Ishiguro et al. (U.S. Patent No. 5,883,958, hereinafter "Ishiguro") in view of Yagawa et al. (U.S. Patent No. 6,751,598, hereinafter "Yagawa").

Applicants respectfully submit that independent Claims 9, 10, 11, 14 and 15 state novel features clearly not taught or rendered obvious by the applied references.

Before turning to the outstanding prior art rejections, it is believed that a brief review of the present invention would be helpful.

Claim 11 relates to an information processing method for preventing unauthorized operations from being performed on content data. The content data is stored in a first memory, and includes management information (e.g., content identifier, artist name, etc.) and calculation information (e.g., MAC value, encryption key, etc.). A sequential number related to the content data is stored and updated upon each operation (e.g., copy, etc.) performed on the stored content. Calculation information is then calculated based on the management information and a latest stored sequential number. After receiving a request to perform an operation on the content data, the sequential number is incremented, and the management information is updated. Then, the calculation information included in the content, the management information included in the content, and the latest sequential number from the second memory are read, and the calculation information included in the content read in the reading step is compared with calculation information calculated in the calculating step. An

operation on the content is then controlled based on the result of the comparison between the two values (e.g., if the two values match, then the data has not been tampered with).

Such an operation prevents a user from modifying the management data (e.g., modifying the incremental value indicating a number of reproductions) to manipulate the data in an unauthorized manner.

Turning to the applied reference, Ishiguro describes a method and device for tamper resistant video data playback in which multiple sets of public keys, used to decrypt the video data, are retrieved from the DVD-ROM (2).[1] Each public key includes a corresponding "flag" indicating whether the key is valid. A controller (20) of the disc drive extracts the public key and associated flag relevant to the ID received from the controller (30).[2] The controller (20) then verifies the validity of the flag of the public key.

However, as admitted in the outstanding Office Action, Ishiguro does not describe or suggest "means for setting a sequential number corresponding to the content data, the sequential number incremented by one when an operation is preformed on the content data stored in the means for storing content data; means for calculating a hash value corresponding to the content data by performing a predetermined calculation using at least a part of the management data associated with the content data and the sequential number."

The outstanding Office Action relies on Yagawa as curing this above noted deficiency in Ishiguro.

Yagawa describes a system in which the use of an illegal copy of a digital content can be prevented.[3]

The outstanding Office Action states on page 3, in item 9 that col. 8, lines 52-57 of Yagawa describes calculating a hash value corresponding to the content data by performing a

[1] Ishiguro at Abstract, and col. 3, lines 54-65.
[2] Id. at col. 4, lines 6-15.
[3] Yagawa, abstract.

predetermined calculation using at least a part of the management data associated with the content data and the sequential number, as is similarly recited in Claims 9, 10, 11, 14 and 15.

Col. 8, lines 52-57 of Yagawa states, "In the case where it is determined through a keyword or hash function matching or the like that a predetermined relation is satisfied between both the keys or a matching between both the keys is obtained, the process is continued (step 437)." In other words, col. 8, lines 52-57 of Yagawa describes discriminating a key match in a system in which a storage medium certification unit 43 judges whether or not the key exists in the ROM area of the storage medium 11 and has a correct code.

However, as can be seen clearly above, Yagawa does not describe or suggest calculating a hash value by performing a predetermined calculation using at least a part of the management data associated with the content data and the sequential number. Although Yagawa describes a distribution control unit that updates the number of times a work is distributed,[4] Yagawa does not describe or suggest calculating a hash value using management data associated with the content data and the sequential number.

Therefore Applicants respectfully submit that Claims 9, 10, 11, 14 and 15 and claims depending therefrom patentably distinguish over Ishiguro and Yagawa.

Therefore, the applied references fail to provide a *prima facie* case of obviousness with regard to any of these claims.

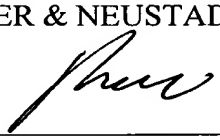
Accordingly, Applicants respectfully requests the rejection of Claims 9-17 under 35 U.S.C. § 103 be withdrawn.

[4] Yagawa, fig. 8.

Consequently, in view of the present Amendment and in light of the foregoing comments, it is respectfully submitted that the invention defined by Claims 9-17 is patentably distinguishing over the applied references. The present application is therefore believed to be in condition for formal allowance and an early and favorable reconsideration of the application is therefore requested.

Respectfully submitted,

OBLON, SPIVAK, McCLELLAND,
MAIER & NEUSTADT, P.C.



Bradley D. Lytle
Attorney of Record
Registration No. 40,073

Customer Number
22850

Tel: (703) 413-3000
Fax: (703) 413 -2220
(OSMMN 06/04)

I:\ATTY\JL\203742US\203742US_AM.DOC